UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/942,396	08/30/2001	Sylvia Halasz	2000-0249	9706

7590 05/04/2006

Mr. S.H. Dworetsky
AT&T Corp
One AT&T Way
Room 2A-207
Bedminster, NJ 07921

EXAMINER	
FIELDS, COURTNEY D	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 05/04/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/942,396	HALASZ ET AL.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 February 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-51 are pending.

Response to Arguments

1. Applicant's arguments filed 06 February 2006 have been fully considered but they are not persuasive.

2. Referring to the rejection of claim 1, the Applicant contends that the prior art, (Ricciulli) does not teach nor disclose predetermined time interval nor probability distribution of arrival times (i.e., arrival time of one packet compared to arrival time of another packet). The Examiner respectfully disagrees and asserts that Ricciulli teach in Figure 2, predetermined time interval wherein The server sends out a SYN-ACK message to each return address for each of these SYN packets. The SYN-ACK message is simply lost in the network. The server never receives any ACK messages back because there are no client systems at the spoofed return addresses. The server, therefore, keeps waiting in vain for an ACK message and may keep a queue entry allocated, for example, for several seconds. In sending out the SYN-ACK messages, the server uses up memory resources and queues a half-open connection for each spoofed SYN message. After a predetermined waiting period, the server times out waiting for a SYN message and closes the corresponding half-open connection (See Column 1, lines 50-62) Ricciulli teaches distribution of arrival times wherein a random drop scheme can be modeled as R.sub.good and T are the average rate of arrival and the average round-trip time of all clients attempting a connection to the server, q is the size of the connection pending queue, and R.sub.bad is the constant rate at which SYN

packets with spoofed source addresses arrive to the server. The expression (1-1/q) is the probability that a new arrival will not cause an existing entry to be dropped. Because each arrival can be statistically independent, by elevating (1-1/q) to the power of the number of expected arrivals during the servicing of the requests ((R.sub.good +R.sub.bad) T), one can find the probability that a legitimate request will succeed. (See Column 3, lines 65-67, Column 4, lines 8) Furthermore, Ricciulli discloses arrival time of packets wherein a "Linux cookie" embodiment can combine the incoming SYN packet's sequence number, and the source and destination addresses, with a secret number (which is changed at regular intervals), and run them through a one-way hash function. The resulting cookie can be the sequence number of the reply. The reply (SYN-ACK packet) can be then sent to the source, using the cookie. No record may be kept locally of the TCP connection request. If and when the ACK packet arrives from the source address as the third step of the handshake process, the sequence number of the received message can be used to authenticate the source. If the source can be properly authenticated, the connection can be established; otherwise, the ACK packet can be discarded (See Column 7, lines 30-42)

3. Referring to the rejection of claims 5 and 35, the Applicant contends that the prior art, (Ricciulli) does not teach nor disclose calculating a difference value in the arrival times of the first request and second request at the host device for comparing the difference value to the predetermined time interval. The Examiner respectfully disagrees and asserts that Ricciulli teach packets transmitted throughout the network wherein a running total can be kept of outstanding SYN packets (SYN packets that have not yet

been acknowledged by the clients 340) and a TCP reset message can be sent by the sending component to the servers 330 in order to keep the total of all outstanding SYN packets under a predetermined threshold value. In one embodiment, when the computer 310 captures a packet that indicates an acknowledge (ACK) from a client 340, the client source or return address is recorded and used to avoid capturing future packets from that client. In some embodiments, additional computers 310 can be deployed at various network locations, permitting scaling upward to the meet the requirements of the servers 330 requiring protection from denial of service attacks (See Column 5, lines 1-18)

4. Referring to the rejection of claims 6 and 36, the Applicant contends that the prior art, (Ricciulli) does not teach nor disclose a network control center. The Examiner respectfully disagrees and asserts that Ricciulli teach a network which includes hardware and software and control various devices within a network wherein some embodiments can protect multiple servers by capturing all, or many, packets destined to each of the protected servers, and sending packets to each of the protected servers. Some embodiments can be implemented in user memory space, and/or without requiring modifications to the software and/or hardware of the servers and/or client(s). Various embodiments can coexist with other SYN flooding defense systems. Some embodiments can be distributed across multiple detached computers, each assigned a distinct set of one or more servers and/or one or more port numbers to protect (See Column 4, lines 27-46)

Furthermore, Ricciulli discloses various embodiments having different types of the network, such as a local area network, wide area network, or an internetwork. In one embodiment, if the network is a local area network, the computer 310 and the servers 330 can share a same broadcast network, such as the same Ethernet segment. The computer 310 and the servers 330 are coupled to the one or more clients via a network. Various embodiments have different types of the network. The shown embodiment uses for the network one example of an internetwork, the Internet. The computer implements a random "early drop" scheme. The servers may or may not be aware of the random "early drop" scheme. Various embodiments can position a packet sniffer component, a random selection component, and a sending component at one or more software modules executing on one or more circuits, and/or at one or more circuits without software. The circuits can be electrical, magnetic, and/or optical, and can be positioned at one or more computers. (See Column 4, lines 49-67)

5. Therefore, the rejection of claims 1-51 are maintained in view of the reasons above and in view of the reasons below.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-51 are rejected under 35 U.S.C. 102(e) as being anticipated by Ricciulli (US Patent No. 6,816,910).

Referring to the rejection of claims 1,13, 20, 23-24, and 31, Ricciulli discloses a method of protecting a host device from a disruptive event, comprising the steps of:

receiving a first request from a client for starting a first data connection (See Column 1, lines 32-38)

receiving a second request from the client for starting a second data connection (See Column 1, lines 38-45)

determining whether the first request and the second request have arrived at the host device within a predetermined time interval, the predetermined time interval being based on a probability distribution function of the arrival times of previous requests for starting data connections received at the host device from a given originating location (See Column 5, lines 1-10)

and responsive to the step of determining, denying the second data connection to the client (See Column 5, lines 22-40)

Referring to the rejection of claims 2,21, and 32, Ricciulli discloses the claimed limitation wherein the step of denying further comprises the step of preventing transmission of a synchronize message to the client (See Column 7, lines 16-23)

Referring to the rejection of claims 3 and 33, Ricciulli discloses the claimed limitation wherein the step of storing the first request from the client (See Column 5, lines 62-63)

Referring to the rejection of claims 4 and 34, Ricciulli discloses the claimed limitation wherein the step of storing an originating address of the client (See Column 5, lines 62-63)

Referring to the rejection of claims 5 and 35, Ricciulli discloses the claimed limitation wherein the step of calculating a difference value in the arrival times of the first request and second request at the host device for comparing the difference value to the predetermined time interval (See Column 5, lines 22-40)

Referring to the rejection of claims 6 and 36, Ricciulli discloses the claimed limitation wherein the step of transmitting a signal to a network control center for taking corrective action against the client (See Column 3, lines 44-58)

Referring to the rejection of claims 7,37, 41, and 49, Ricciulli discloses the claimed limitation wherein the step of barring the client access to the host device by downloading from the network control center appropriate commands to the server and appropriate commands to specific switching devices in the network (See Column 6, lines 1-7)

Referring to the rejection of claims 8,38,42,50, and 51 Ricciulli discloses the claimed limitation wherein the step of signaling the host device to shut down and the step of sending commands from the network control center to one or more standby servers to take over the processing functions performed by the host device that was shut down (See Column 4, lines 47-67)

Referring to the rejection of claims 9,22, 39, and 43 Ricciulli discloses the claimed limitation wherein the step of proceeding with establishment of the second data

connection if the first request and the second request have arrived at the host device outside of the predetermined time interval (See Column 5, lines 22-40)

Referring to the rejection of claim 10, Ricciulli discloses the claimed limitation wherein the step of transmitting a synchronize message to the client (See Column 5, lines 1-18)

Referring to the rejection of claim 11, Ricciulli discloses the claimed limitation wherein the step of storing an originating address of the client and the arrival time of the second request (See Column 5, lines 62-67)

Referring to the rejection of claim 12, Ricciulli. discloses the claimed limitation wherein the disruptive event is a flooding attack (See Column 1, lines 46-49)

Referring to the rejection of claims 14,25, and 45 Ricciulli discloses the claimed limitation wherein the step of denying the request comprises preventing transmission of a synchronizing message to the originating address (See Column 7, lines 16-23)

Referring to the rejection of claims 15,26, and 46 Ricciulli discloses the claimed limitation wherein the step of saving the originating address and the arrival time of the initializing request (See Column 6, lines 44-53)

Referring to the rejection of claims 16,27, and 47 Ricciulli discloses the claimed limitation wherein the step of denying the request further comprises closing a connection for the data transmission session (See Column 1, lines 49-64)

Referring to the rejection of claims 17,28, and 48 Ricciulli discloses the claimed limitation wherein the step of calculating a difference value in arrival times of the

initializing request and the previously received initializing request from the originating address (See Column 5, lines 22-40)

Referring to the rejection of claims 18 and 29, Ricciulli discloses the claimed limitation wherein the step of transmitting a signal to a network control center responsive to the step of denying (See Column 6, lines 54-65)

Referring to the rejection of claims 19 and 30, Ricciulli discloses the claimed limitation wherein the step of monitoring a plurality of data packets arriving at the host device so as to generate a probability distribution of the arrival times of a plurality of initializing requests from the originating address (See Column 4, lines 27-46)

Referring to the rejection of claims 40 and 44, Ricciulli discloses a method of protecting a host device from a flooding event, comprising the steps of:

receiving a first request from a client for starting a first data connection (See Column 1, lines 32-38)

receiving a second request from the client for starting a second data connection (See Column 1, lines 38-45)

determining whether the first request and the second request have arrived at the host device within a predetermined time interval, the predetermined time interval being based on a probability distribution function of the arrival times of previous connection establishment requests received at the host device (See Column 5, lines 1-10)

and responsive to the step of determining, signaling a network control center (See Column 3, lines 44-58)

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cdf
April 30, 2006

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER